情報ネットワーク学　7月5日レポート

2017/07/09

37-176843 中川大海

2016年からメディアを賑わしている「Mirai」について調べなさい。

- Miraiとは何か
- 具体的な事例
- 対策

など

Miraiとは、ボットネットを構成するマルウェアのことである。「C&C」と呼ばれる管理端末を操作することで、感染させた機器から攻撃対象のサーバーに対して大量のパケットを送信させるという一般的な特徴に加え、ボット化の対象がLinux上で動作するIoTデバイスであったことが大きな特徴で、市場まれに見る大規模なボットネットによる攻撃を可能にした。ランダムなIPアドレスに対してログイン情報を辞書攻撃する手法により、PCほどの性能はないものの大量に存在するインターネットに接続したIoTデバイスが感染してしまい、被害が拡大した。
具体的な事例としては、2016年9月の著名セキュリティ情報ブログ「Krebs on Security」に対するDDoS攻撃や、フランスのホスティングサービス「OVH」に対する1Tbpsを超えるDDoS攻撃などがある。
直接的な対策としては、IoTデバイスのパスワードなどをデフォルトのものから変更するというものがあるが、そもそも利用者がパスワードを認知できなかったりハードコーディングされていて変更できない場合は、メーカーやベンダー側がデバイスの設計の段階から変更するという対策が必要になる。また、平文の通信のため、SSHなどで通信を暗号化することなども有効と考えられる。